PREVENTING ATTACKS IN A DATA PROCESSING SYSTEM

ABSTRACT

A method and apparatus for facilitating reduction in successful attacks on a monitored data processing system, such as a host computer. An intrusion detection system comprises a host or application based sensor for detecting code based intrusions with a relatively low false-positive rate. Malicious code strings related to a detected intrusion are identified, extracted and forwarded to a pattern filter located in the monitored data processing system to prevent further intrusions using said malicious code strings. The malicious code strings may be forwarded to a response server for assembling sets of similar malicious code strings for which signatures are generated to permit identification of all malicious code strings contained in a set. The generated signatures are then distributed to monitored and/or monitoring systems of a protected network to prevent further intrusions using the malicious code strings and variations thereof.